EXHIBIT 1

Expert Report of Scott A. Kraemer

9793 W. Hedge Hog PL, Peoria AZ 85383.

Background and introduction

On or about April 1, 2023[date], I was engaged by Defendants Phoenix Digital Group LLC ("Phoenix Digital") and James May ("Mr. May") to examine and opine on issues with regard to the matter styled Bungie, Inc. v. AIMJUNKIES.COM, et al, W.D. WA case no. 2:21-cv-811-TSZ. Specifically, I was asked to review documents and potentially write one or more reports and/or declarations and to testify as an expert witness in this action with regard to the Counter Claims made by Phoenix Digital and Mr. May in this matter concerning (1) whether forensic evidence appears to support the conclusion that Plaintiff Bungie, Inc. ("Bungie") reverse engineered, de-compiled and/or otherwise analyzed a certain "loader" software product distributed by Phoenix Digital; and (2) whether Bungie appears from the evidence I reviewed to have accessed certain private files on the computer of Mr. May.

My background with respect to the matters at hand

My name is Scott A. Kraemer and I have been asked to write a report discussing some of the issues involved in this matter. Specifically, within the limits of available time and information, I have been asked to provide opinions related to actions apparently taken by Bungie in the course of investigating Phoenix Digital and James May, and whether such actions violate the Terms of Service of Phoenix Digital and/or Bungie. I specifically have been asked to review and analyze certain documents produced by Bungie and opine as to what those documents reflect and whether those documents suggest that Bungie engaged in such activities as reverse engineering, decompiling or otherwise improperly accessing the technology at issue in this case.

My experience dates back to 1990 when I entered the United States Marine Corps and received training to become Small Systems Specialist. I began C++ coding during this time. I exited the Marine Corps and became a Certified Banyan Engineer, and later a Microsoft Certified Engineer and have been in the Information Technology field for 25+ years under fortune 500 companies. I began reverse engineering as a hobby that turned into a website for reverse engineering online video gamesfor 8 years. I am extremely familiar with decompiling, attaching debuggers, and memory

editing programs that give video game players advantages in games. I retired from programming and reverse engineering in late 2017.

The Relevant Issues

My understanding of the relevant issues is based on my review of the Amended Counterclaims filed in this action on November 21, 2022, and related documents.

My understanding is that Defendant James May has asserted counterclaims alleging that Bungie, without his knowledge, authorization, or permission, accessed certain files on his personal computer in violation of various laws.

My further understanding is that Defendant Phoenix Digital has asserted a counterclaim alleging that Bungie violated Phoenix Digital's Terms of Service by reverse engineering and otherwise analyzing Phoenix Digital's "loader" software in violation of those Terms of Service.

I have been asked to render an opinion as to whether documents provided, and admissions made, by Bungie tend to show that (1) Bungie accessed Mr. May's personal computer files in excess of the authority granted to Bungie by Mr. May, and (2) Bungie acessed Phoenix Digital's "loader" software beyond any authority granted by Phoenix Digital's Terms of Service.

Summary of my conclusions.

Based on my review of certain documents (to be described in detail below) produced in this matter by Bungie, it is my conclusion and opinion that:

1. These documents, and in particular Bungie production documents BUNGIE_WDWA_0000410, BUNGIE_WDWA_0000416, BUNGIE_WDWA_0000421 and BUNGIE_WDWA_0000368, show that Bungie reverse engineered the AimJunkies' Cheat Loader and process flow, dumped crucial proprietary information on how the AimJunkies Cheat Loader and cheat injector work, and accessed the methods and IP addresses of the AimJunkies servers, all in violation of the plain meaning of the applicable Terms of Service put in place by Defendant Phoenix Digital Group LLC.. The Expert Report from Steven Guris lists in detail how he reverse engineered AimJunkies' Cheat Loader on Page 26-30 with images of the loader decompiled.

2. The Expert Witness Report from Steven Guris lists in detail how he reversed engineered the AimJunkies Cheat Loader on Page 26-30 with images of the loader decompiled and gave analysis of his findings.

3. These documents, including but not limited to Bungie production document BUNGIE_WDWA_

0000409, show that Bungie accessed Mr. May's computer files beyond the scope authorized by the plain language of Bungie's Limited Software License Agreement and Privacy Policy. In particular, it is my opinion that these documents produced by Bungie in this action relating to Bungies "Findings of James Mays Files," show that the category "GameCheats.AimJunkies binary found" was accessed outside the games own directory by a process other than the code-script entitled "Reverse Engineer Tool Attached," and beyond the scope of the authorization granted by Mr. May.

Documents reviewed and relied upon

In the course of forming my opinions, I was provided with and reviewed the following documents provided to me by counsel for the Defendants in this matter:

BUNGIE_WDWA_0000002 "Highly Confidential".pdf (Bungie of sample Source Code of x number of functions.)

BUNGIE_WDWA_0000251 "Highly Confidential".pdf (Bungie of sample Source Code of x number of functions.)BUNGIE_WDWA_0000368 "Highly Confidential".pdf (Appears to be a dump of notepad.exe with strings, section data, and encrypted data.)

BUNGIE_WDWA_0000409.XLSX (James May Data.)

BUNGIE_WDWA_0000410 "Highly Confidential).pdf AimJunkies Cheat Analysis Document

BUNGIE_WDWA_0000412_Highly Confidential – Attorney Eyes' Only (CSV process Dump of notepad.exe.)

BUNGIE_WDWA_0000483.pdf Weekly Game Security Report - 17th January 2020

BUNGIE_WDWA_0000488.pdf Weekly Game Security Report - 24th January 2020

BUNGIE_WDWA_0000493.pdf Game Security Report - 11/18/19 - 1/10-20

BUNGIE_WDWA_0000497.pdf Game Security Report week of 11/4/2019

BUNGIE_WDWA_0000518.pdf Emails relating to RE: Destiny Game Security Advisors Weekly Sync - June 29th, 2020

BUNGIE_WDWA_0000522.pdf Emails relating to RE: Destiny Game Security Advisors Weekly Sync - June 29th, 2020

BUNGIE_WDWA_0000525.pdf Emails relating to RE: Destiny Game Security Advisors Weekly Sync - June 29th, 2020

BUNGIE_WDWA_0000528.pdf Emails relating to RE: Destiny Game Security Advisors Weekly Sync - June 29th, 2020

BUNGIE_WDWA_0000536.pdf Emails relating to Game Security Report week of 10/21/2019 - Useless

BUNGIE_WDWA_0000551.pdf Weekly Game Security Report - 24th January 2020

BUNGIE_WDWA_0000552.pdf Weekly Game Security Report - 24th January 2020

BUNGIE_WDWA_0000597.pdf

Bungie Limited Software License Agreement dated March 6, 2020.

Bungie Privacy Policy dated January 21, 2020.

Phoenix (AimJunkies) Terms of Service

Amended Answer and Counterclaims dated November 21, 2022.

Expert Report of Steven Giuris.

Exhibits A, B, C and D to the Amended Counterclaim filed November 21, 2022.

Basis and reasons for my opinions

I am basing my opinion solely on the contents of the documents provided and my knowledge as to what these documents reasonably demonstrate, show and mean from a technical standpoint.

With respect to certain of the documents Bungie has provided in this matter, my conclusions and basis for my conclusions are as set out below:

BUNGIE_WDWA_0000368. This document appears to be a memory dump of notepad.exe. The only way to obtain such document is to attach a tool or debugger to dump the contents of it. As this is a document prepared and produced by Bungie, it is apparent that Bungie, or someone operating on Bungie's behalf, attached the tool or debugger.

BUNGIE_WDWA_0000410. This document discusses obtaining the cheat metholdology, and how to initiate setting up the cheat loader. This document also specifies attempts to detect it, as made apparent in part from the quote below:

"Stage 1: The clear sign would be the IP connections 172.67.73.48 and 104.26.1.138. To

establish these https connections the cheat loader first injects itself into notepad.exe".

This sentence gives the IP addresses of where the cheat communicates with (Aim Junkies Servers). To get these IP addresses either a tool for monitoring network traffic from a PC using the AimJunkies Cheat Loader and subsequent Notepad process must have been used or the Cheat Loader/or Notepad was decompiled. This information is not freely available to keep DDOS attacks down.

BUNGIE_WDWA_0000412. This document shows that Bungie attached "Process Monitor" by SysInternals to the notepad process to monitor its Process and Thread activity and dumped the activity to a csv file. While not very useful, this is an attempt to find out what AimJunkies Cheat is doing.

Counterclaim #2

MD5 Hash.

You will see Bungie used a MD5 Hash on all of the James Files found. For Example in the Exhibit C Document

\??\g:\work files\reclass\x64\plugins\reclasskernel64.sys (8D98DB3A27112A9C92558FF90A1D6206)

g:\work files\reclass\x64\reclass.net.exe (360B1FE16603C1106CD8DEF992846B1B

The 32 length Numbers and Letters in Parenthesis is a MD5 Hash.

What is MD5?

MD5 (message-digest algorithm) is a cryptographic protocol used for authenticating messages as well as content verification and digital signatures. MD5 is based on a hash function that verifies that a file you sent matches the file received by the person you sent it to. Previously, MD5 was used for data encryption, but now it's used primarily for authentication.

How does MD5 work?

MD5 runs entire files through a mathematical hashing algorithm to generate a signature that can be matched with an original file. That way, a received file can be authenticated as matching the original file that was sent, ensuring that the right files are the unmodified originals.

It is my opinion that the technological evidence showed Bungie searched and found files and used a MD5 Hash Generator to access James Mays Files to Generate the Hash. The MD5 Tool/API they used read the full contents of the file to generate and produce the hash values.

System Drivers

The System Drivers found in Exhibit C Example \??\g:\work files\reclass\x64\plugins \reclasskernel64.sys (8D98DB3A27112A9C92558FF90A1D6206)

System Drivers are loaded into a computer system's Kernel and not attached to the game. The Drivers contain no cheat codes for Destiny 2 or any other cheat. These Drivers are Utility Tools used by Phoenix Digital Group. VirusTotal.com shows this file to contain no detected malware or being flagged for malicious content. This specific driver file was first submission to VirusTotal.com on

2022-03-08.

Exhibit D to Amended Counterclaims.

Bungie shows they found "(C:\Users\james\Desktop\ReClass.NET-KernelPlugin-master\bin \ReClassKernel64.pdb)." This file is a symbols / Debug file used when compiling ReClassKern64.sys. A system driver, would never be attached to the game, and was apparently located by other means undertaken by Bungie, which is not explained in Exhibit D or BUNGIE_WDWA_0000409.XLSX by column identification "AimJunkies binary found".

It is my opinion Bungie searched for and accessed these private files and system drivers outside of the Destiny 2 game directory structure and into personal space.

Exhibits
As I understand the various documents I have identified above, including those marked "Confidential" and "Highly Confidential" are already in the possession of Bungie and have previously been filed under seal with the Court, I am not listing those documents as exhibits here. I may, however, use those documents as exhibits if I am called upon to testify before the Court or Jury.

Qualifications and publications
A copy of my resume accompanies this report. I have not had any publications in the last ten years.

List of prior cases
None.

Compensation
I am being compensated by Defendants James May and Phoenix Digital at a rate of $75 per hour.

DocuSigned by:
Scott A. Kraemer
954A15DD9B19405...

Scott A Kraemer

June 12, 2023